US 20170127275A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2017/0127275 A1

Jones-McFadden et al. (43) Pub. Date: May 4, 2017

(54) **INTEGRATED FULL AND PARTIAL SHUTDOWN APPLICATION PROGRAMMING INTERFACE**

(71) Applicant: **BANK OF AMERICA CORPORATION**, Charlotte, NC (US)

(72) Inventors: **Alicia C. Jones-McFadden**, Fort Mill, SC (US); **Elizabeth S. Votaw**, Potomac, MD (US)

(21) Appl. No.: **14/928,498**

(22) Filed: **Oct. 30, 2015**

Publication Classification

(51) **Int. Cl.**

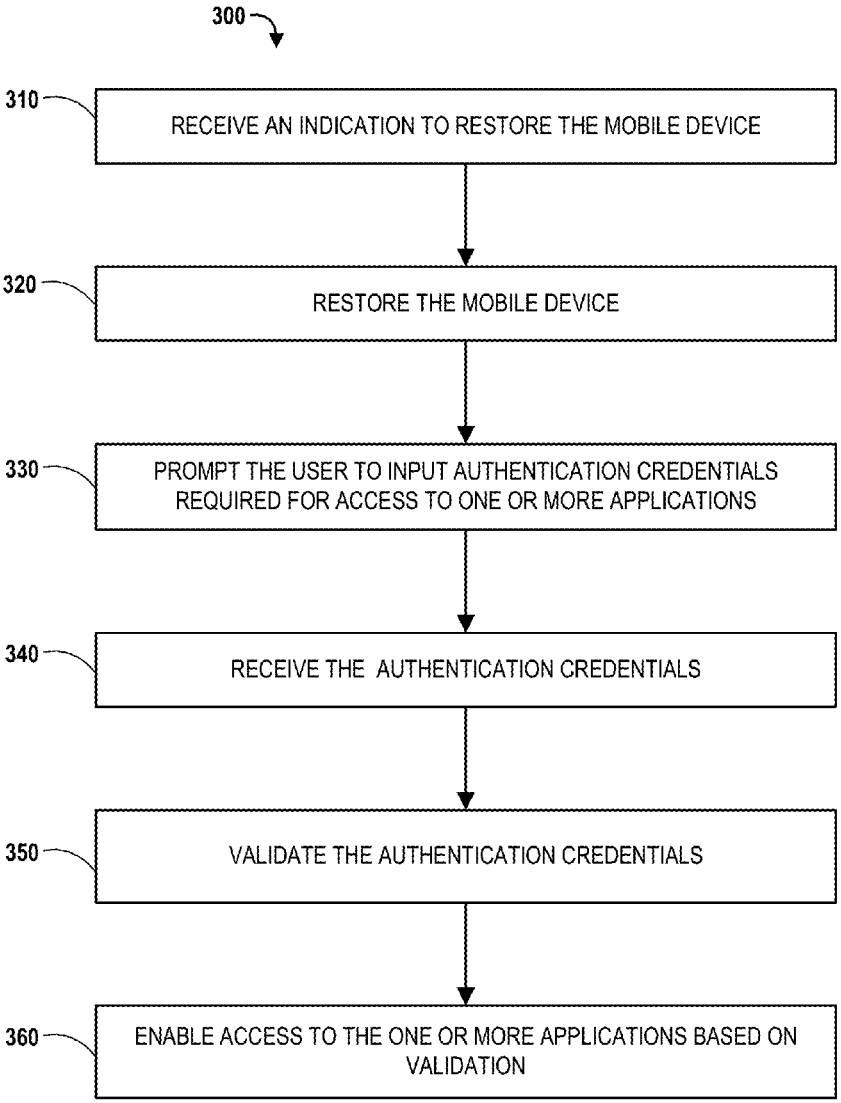
H04W 12/06	(2006.01)
G06F 9/445	(2006.01)
H04L 29/06	(2006.01)

(52) **U.S. Cl.**

CPC ***H04W 12/06*** (2013.01); ***H04L 63/083*** (2013.01); ***G06F 8/62*** (2013.01)

(57) **ABSTRACT**

The present disclosure describes an integrated full and partial shutdown application programming interface. Embodiments herein disclosed include receiving an indication that a mobile device of a user is compromised. Further embodiments identify one or more applications associated with the mobile device and remotely access the mobile device to perform a switch-off of the one or more applications. The switch-off may include logging the user out of the one or more applications before removing the one or more applications from the mobile device.



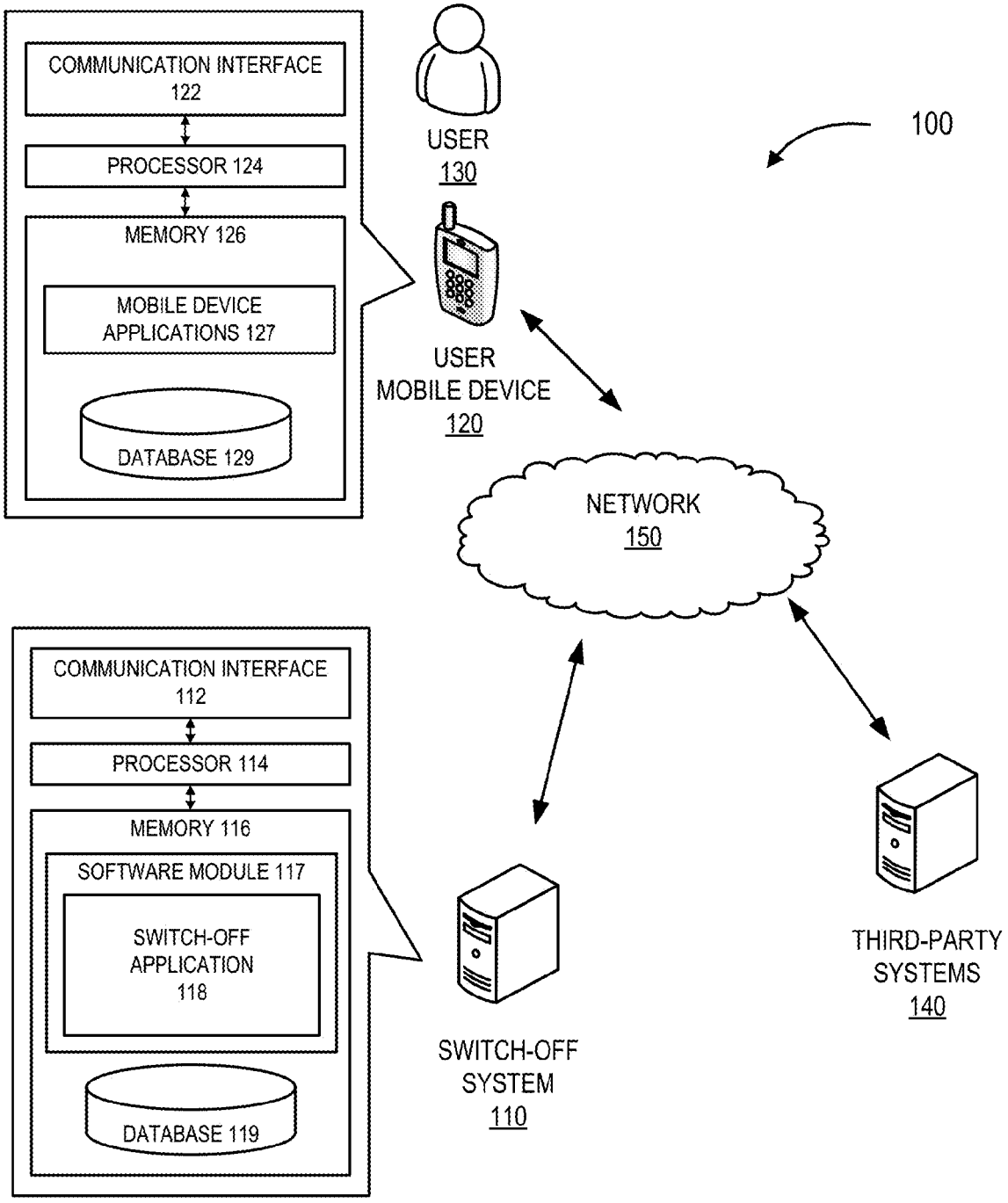

COMMUNICATION INTERFACE 122
PROCESSOR 124
MEMORY 126
MOBILE DEVICE APPLICATIONS 127
DATABASE 129
USER 130
100
USER MOBILE DEVICE 120
NETWORK 150
COMMUNICATION INTERFACE 112
PROCESSOR 114
MEMORY 116
SOFTWARE MODULE 117
SWITCH-OFF APPLICATION 118
DATABASE 119
SWITCH-OFF SYSTEM 110
THIRD-PARTY SYSTEMS 140

FIG. 1

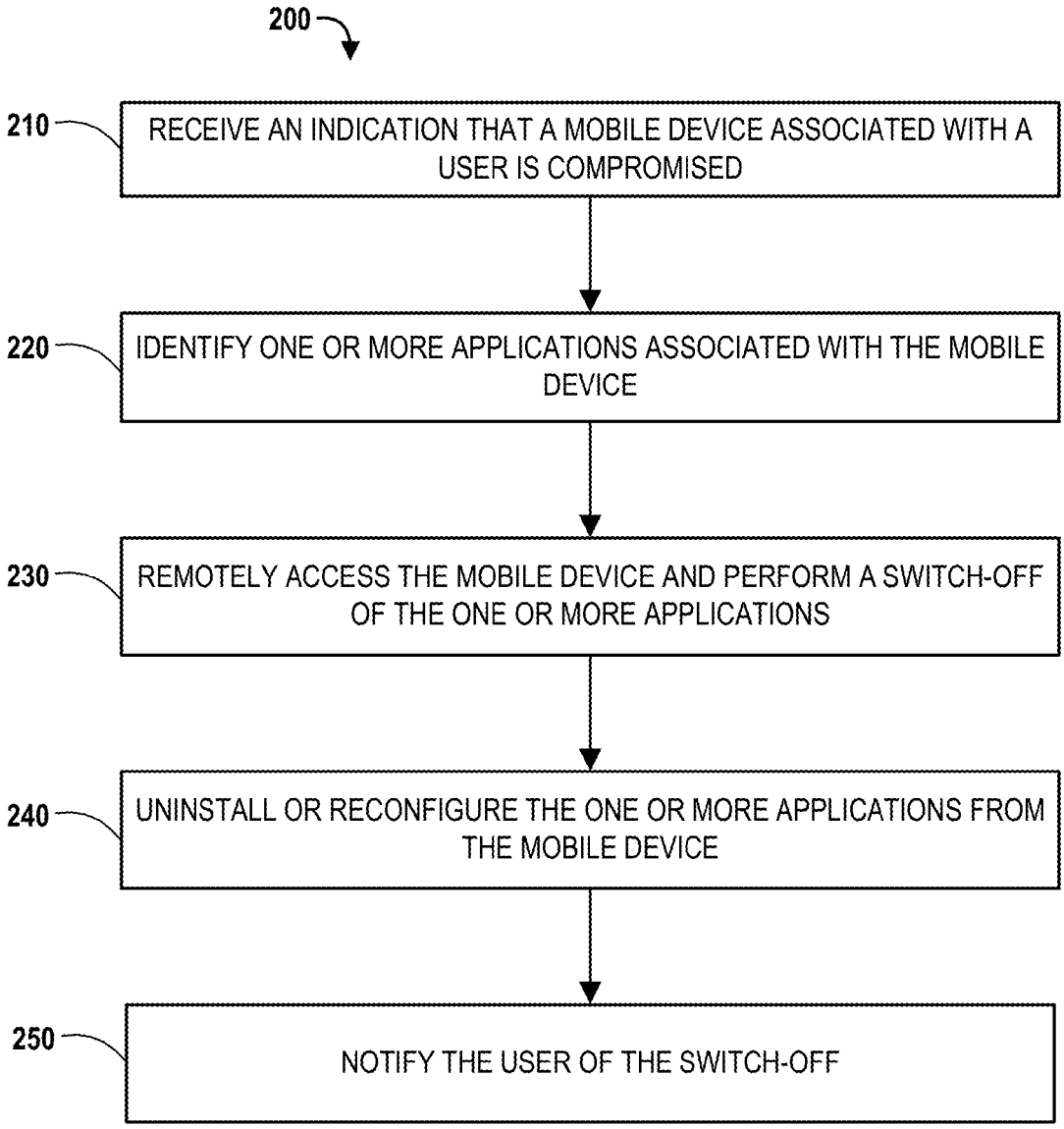

200
210
RECEIVE AN INDICATION THAT A MOBILE DEVICE ASSOCIATED WITH A USER IS COMPROMISED
220
IDENTIFY ONE OR MORE APPLICATIONS ASSOCIATED WITH THE MOBILE DEVICE
230
REMOTELY ACCESS THE MOBILE DEVICE AND PERFORM A SWITCH-OFF OF THE ONE OR MORE APPLICATIONS
240
UNINSTALL OR RECONFIGURE THE ONE OR MORE APPLICATIONS FROM THE MOBILE DEVICE
250
NOTIFY THE USER OF THE SWITCH-OFF

FIG. 2

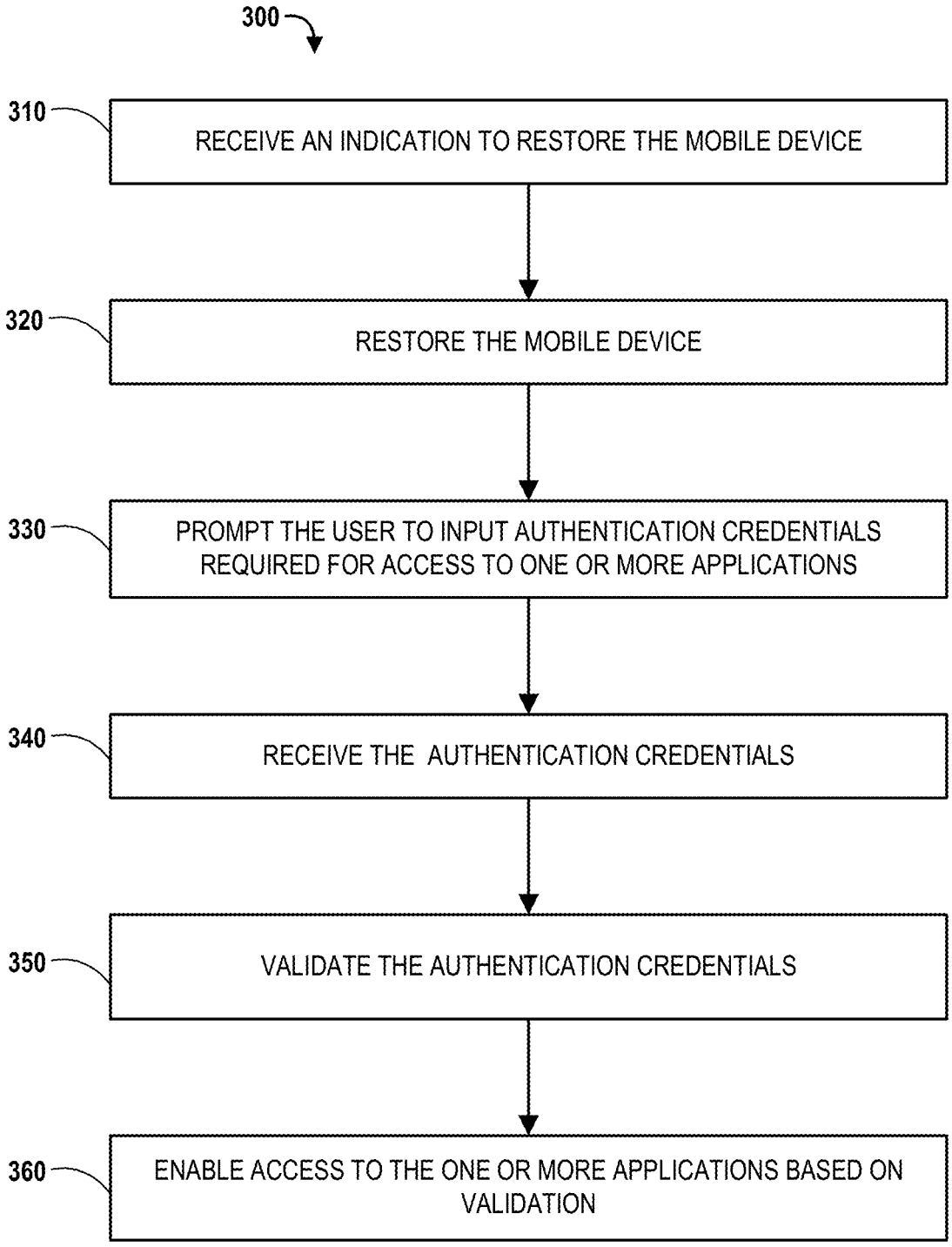

300
310
RECEIVE AN INDICATION TO RESTORE THE MOBILE DEVICE
320
RESTORE THE MOBILE DEVICE
330
PROMPT THE USER TO INPUT AUTHENTICATION CREDENTIALS REQUIRED FOR ACCESS TO ONE OR MORE APPLICATIONS
340
RECEIVE THE AUTHENTICATION CREDENTIALS
350
VALIDATE THE AUTHENTICATION CREDENTIALS
360
ENABLE ACCESS TO THE ONE OR MORE APPLICATIONS BASED ON VALIDATION

FIG. 3

INTEGRATED FULL AND PARTIAL SHUTDOWN APPLICATION PROGRAMMING INTERFACE

FIELD OF THE INVENTION

[0001] This disclosure generally relates to systems and methods for an integrated full and partial shutdown application programming interface (API).

BACKGROUND

[0002] Mobile technology allows users to download a variety of applications and functions to their mobile devices. A mobile application may allow users to remotely access to their personal information and perform some actions based on the information. When such a mobile device is misplaced or misappropriated, then the user's information can be jeopardized. Merely uninstalling the applications from a mobile device may not effectively prevent a third party from gaining access to the user's profile by re-installing the application on the mobile device. As such, there exists a need for effective protection of user information when their mobile devices are misplaced or misappropriated.

SUMMARY OF THE INVENTION

[0003] The following presents a summary of certain embodiments. This summary is not intended to be a comprehensive overview of all contemplated embodiments, and is not intended to identify key or critical elements of all embodiments nor delineate the scope of any or all embodiments. Its sole purpose is to present certain concepts and elements of one or more embodiments in a summary form as a prelude to the more detailed description that follows.

[0004] Systems, computer-implemented methods, and computer program products are described herein that provide for embodiments of an integrated full and partial shutdown application programming interface. With reference to the system, a computer apparatus that comprises at least one processor and a memory may be a part of the system. Additionally, the system may comprise a software module, stored in the memory, comprising computer readable code, executable by the processor, and configured to execute a plurality of steps. Some embodiments of the system comprise receiving an indication to perform a switch-off for a mobile device associated with a user. The system may identify one or more applications associated with the mobile device and remotely access the mobile device to perform the switch-off of the one or more applications. In some embodiments, the switch-off comprises logging the user out of the one or more applications and uninstalling or reconfiguring the one or more applications from the mobile device, wherein uninstalling comprises removing all or part of the one or more applications from the mobile device, and wherein reconfiguring comprises disabling access to the one or more applications.

[0005] In some embodiments of the system, the switch-off further comprises confirming that the user is logged out of the one or more applications prior to uninstalling or reconfiguring the one or more applications from the mobile device.

[0006] In some embodiments, the system may restore the mobile device to an original state, wherein the original state is a state prior to the switch-off, wherein restoring comprises reinstalling the all or part of the one or more applications that were removed from the mobile device. Additionally, the system may prompt the user to input authentication credentials required for access to the one or more applications and receive, from the user, the required authentication credentials. Furthermore, the system may validate the authentication credentials and re-establish, based on validating the authentication credentials, the user's access to the one or more applications.

[0007] In some embodiments of the system, the authentication credentials comprise one or more of a username, a password, a passcode, a personal identification number (PIN), security questions, biometric indicia, device info associated with the mobile device, and financial account information of the user. In some embodiments of the system, the software module is further configured to notify the user of the switch-off.

[0008] In some embodiments of the system, the indication to perform the switch-off comprises an indication that the mobile device is misplaced or lost, that the one or more applications are misappropriated, or that the mobile device and a wearable device of the user are not co-located.

[0009] In some embodiments of the system, logging the user out of the one or more applications comprises logging the user out of a first authentication tier but not logging the user out of a second authentication tier.

[0010] Computer program product embodiments of the invention may comprise a non-transitory computer readable medium having one or more computer readable programs stored therein, and the computer readable programs, when executed by a computer apparatus, can cause the computer apparatus to perform a plurality of steps.

[0011] To the accomplishment of the foregoing and related objectives, the embodiments of the present invention comprise the function and features hereinafter described. The following description and the referenced figures set forth a detailed description of the present invention, including certain illustrative examples of the one or more embodiments. The functions and features described herein are indicative, however, of but a few of the various ways in which the principles of the present invention may be implemented and used and, thus, this description is intended to include all such embodiments and their equivalents.

[0012] The features, functions, and advantages that have been discussed may be achieved independently in various embodiments of the invention or may be combined with yet other embodiments, further details of which can be seen with reference to the following description and drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0013] Having thus described embodiments of the invention in general terms, reference may now be made to the accompanying drawings:

[0014] FIG. **1** is a block diagram illustrating a system environment including a system for integrated full and partial shutdown API, in accordance with an embodiment of the invention;

[0015] FIG. **2** is a flowchart illustrating a general process for performing a switch-off of applications on a mobile device, in accordance with an embodiment of the present invention; and

[0016] FIG. **3** is a flowchart illustrating a general process for restoring a mobile device, in accordance with an embodiment of the present invention.

DETAILED DESCRIPTION OF EMBODIMENTS OF THE INVENTION

[0017] Embodiments of the present invention will now be described with respect to FIGS. **1-3**. In view of this description, modifications and alterations to these embodiments or implementations will be apparent to one of ordinary skill in the art.

[0018] In the drawings, like reference characters and numbers refer to like elements throughout. Also, the drawings are not necessarily to scale, emphasis instead generally being placed upon illustrating the principles of the invention.

[0019] As may be appreciated by one of skill in the art, the present invention may be embodied as a method, system, computer program product, or a combination of the foregoing. Accordingly, the present invention may take the form of an entirely software embodiment (including firmware, resident software, micro-code and the like) or an embodiment combining software and hardware aspects that may generally be referred to herein as a "system." Furthermore, embodiments of the present invention may take the form of a computer program product on a computer-readable medium having computer-usable program code embodied in the medium.

[0020] In some embodiments, any suitable computer-readable medium may be utilized. The computer-readable medium may be, for example but not limited to, an electronic, magnetic, optical, electromagnetic, infrared, or semiconductor system, apparatus, device, or propagation medium. More specific examples of the computer readable medium include, but are not limited to, the following: an electrical connection having one or more wires; a tangible storage medium such as a portable computer diskette, a hard disk, a random-access memory (RAM), a read-only memory (ROM), an erasable programmable read-only memory (EPROM or Flash memory), a compact disc read-only memory (CD-ROM), or other optical or magnetic storage device; or transmission media such as those supporting the Internet, an intranet, or a wireless network. Note that the computer-readable medium could even be paper or another suitable medium upon which the program is printed, as the program can be electronically captured, via, for instance, optical scanning of the paper or other medium, then compiled, interpreted, or otherwise processed in a suitable manner, if necessary, and then stored in a computer memory. In some embodiments, the system may use a non-transitory computer readable medium. Additionally, in some embodiments, the system may not use a general computing device, but instead may use a specialized computing device specifically designed and configured to carry out the features of the present invention.

[0021] Computer program code for carrying out operations of embodiments of the present invention may be written in an object oriented, scripted or unscripted programming language such as Java, Perl, Smalltalk, C++, or the like. However, the computer program code for carrying out operations of embodiments of the present invention may also be written in conventional procedural programming languages, such as the "C" programming language or similar programming languages. The program code may execute entirely on the user's computer, partly on the user's computer, as a stand-alone software package, partly on the user's computer and partly on a remote computer or entirely on the remote computer or server. In the latter scenario, the remote computer may be connected to the user's computer through any type of network, including a local area network (LAN) or a wide area network (WAN), or the connection may be made to an external computer (for example, through the Internet using an Internet Service Provider).

[0022] Embodiments of the present invention are described below with reference to flowchart illustrations and/or block diagrams of methods, apparatus (systems), and computer program products. It may be understood that each block of the flowchart illustrations and/or block diagrams, and/or combinations of blocks in the flowchart illustrations and/or block diagrams, can be implemented by computer program instructions. These computer program instructions may be provided to a processor of a general purpose computer, special purpose computer, or other programmable data processing apparatus to produce a machine, such that the instructions, which execute via the processor of the computer or other programmable data processing apparatus, create mechanisms for implementing the functions/acts specified in the flowchart and/or block diagram block or blocks.

[0023] These computer program instructions may also be stored in a computer-readable memory that can direct a computer or other programmable data processing apparatus to function in a particular manner, such that the instructions stored in the computer readable memory produce an article of manufacture including instruction means which implement the function/act specified in the flowchart and/or block diagram block(s).

[0024] The computer program instructions may also be loaded onto a computer or other programmable data processing apparatus to cause a series of operational steps to be performed on the computer or other programmable apparatus to produce a computer-implemented process such that the instructions which execute on the computer or other programmable apparatus provide steps for implementing the functions/acts specified in the flowchart and/or block diagram block(s). Alternatively, computer program implemented steps or acts may be combined with operator or human implemented steps or acts in order to carry out an embodiment of the invention.

[0025] The present disclosure provides systems, methods and computer products for integrated full and partial shutdown application program interface (API). Generally, the systems and methods herein disclosed perform a switch-off of one or more applications on a mobile device of a user, after receiving an indication to perform a switch-off. The system generally accomplishes the shut-off task by opening the one or more applications on the user device to log out of the applications. The system may then wipe or otherwise remove the one or more applications from the mobile device. By logging out of these applications before removing the applications from the mobile device, the system prevents a third party user from re-installing the application to the mobile device and automatically being logged in to the application under the user's profile. Of course, the system may include other and additional techniques to accomplish this task, including requiring user authorization to re-establish activation of the mobile device and/or the one or more applications on the mobile device, removing cached data on the mobile device, and the like.

[0026] Referring now to FIG. **1**, a block diagram of a system environment **100** is provided, which includes a switch-off system **110** administrated by a financial institu-

tion, a user mobile device **120** operated by a user **130**, third-party systems **140**, and a network **150**. The switch-off system **110**, the mobile device **120** and third-party systems **140** communicate with one another over the network **150**.

[0027] A "system environment," as used herein, may refer to any information technology platform of an enterprise, for example, a national or multi-national corporation, and may include a multitude of servers, machines, mainframes, personal computers, network devices, front and back end systems, database systems and/or the like.

[0028] A "financial institution," as used herein, refers to any organization, entity, or business unit in the business of moving, investing, or lending money, dealing in financial instruments, or providing financial services. For example, a financial institution may be a commercial bank, a mortgage company, a credit union, an insurance company, a financial consulting firm, an investment company, or the like.

[0029] The term application program interface, or "API," as used herein, refers to a set of programming instructions and standards, or routines and tools for accessing a web-based application. As used herein, the terms "web-based application" and "online application" are interchangeable, both referring to an application that can be accessed through a network connection using an application-level protocol such as the hypertext transfer protocol (HTTP).

[0030] As used herein, the terms "customer" and "user" are interchangeable, both referring to a person who is affiliated with a financial institution herein defined.

[0031] A "third party," as used herein, refers to any business or non-business units, outside the boundary of the financial institution, which provides services, applications and functions to users, such as websites, social networking media, email servers and the like.

[0032] As shown in FIG. **1**, the switch-off system **110** includes a communication interface **112**, at least one processor **114**, and a memory **116**. The memory **116** includes a software module **117** including one or more switch-off applications **118** and a database **119**. The communication interface **112** may encompass one more network interface cards, ports for connection of network devices, Universal Serial Bus (USB) connectors and the like.

[0033] The processor **114** is operatively coupled to the memory **116** and configured to execute the software module **117**. The processor **114** may include a digital signal processor device, a microprocessor device, analog-to-digital converters, digital-to-analog converters, and other support circuits. Control and signal processing functions of the processor **114** may be allocated between these devices according to their respective capabilities. The processor **114** may also include functionality to operate other software programs based on computer executable code thereof, which may be stored, along with the switch-off applications **118**, on the switch-off system **110**.

[0034] The memory **116** may include volatile memory, such as RAM having a cache area for the temporary storage of information. The memory **116** may also include non-volatile memory that may be embedded and/or removable. The non-volatile memory may additionally or alternatively include an Electrically Erasable Programmable Read-Only Memory (EEPROM), flash memory, and/or the like.

[0035] The software module **117** contains computer readable code executable by the processor **114** and includes the one or more switch-off applications **118**. The switch-off applications **118** may perform one or more of the steps and/or sub-steps discussed herein and/or one or more steps not discussed herein.

[0036] It will be understood that the switch-off system **110** may be configured to implement various user interfaces, applications and/or process flow described herein. It will also be understood that, in some embodiments, the memory **116** includes other applications. It will also be understood that, in some embodiments, the switch-off system **110** may be configured to communicate with third-party systems **140**, for example, for purpose of identifying the mobile device **120** and/or the user **130**.

[0037] The database **119** may archive information of users affiliated with the financial institution, such as user profiles for access to one or more online banking applications provided by or associated with the financial institution. The database **119** may also store data/results related to and/or used by the switch-off applications **118**.

[0038] The user mobile device **120**, as shown in FIG. **1**, includes a communication interface **122**, a processor **124** and a memory **126**. The memory **126** also includes one or more mobile device applications **127**, and a database **129**. The one or more mobile device applications **127** may comprise any application for the mobile device accessible by the user **130**, a financial institution, a third party system **140** and/or the switch-off system **110**. The applications may be related to the financial institution, an online banking system, a social media platform, a merchant platform, a gaming platform, and the like. The user mobile device **120** may, by way of example, comprise a personal digital assistant, a personal computer, an electronic notebook, a mobile phone, a tablet computer, a smart wearable device, and the like.

[0039] In some embodiments, the one or more mobile device applications **127** are provided by or associated with the financial institution and include functionality features that allow the user **130** to act on one or more financial accounts associated with the user **130**, for example, transferring funds between the accounts, executing account withdrawals or deposits, processing commercial payments related to online bill-pay or peer-to-peer payments, and the like. The financial accounts associated with the user **130** may include one or more deposit accounts, debit accounts, savings accounts, checking accounts, investment accounts, money market accounts, credit accounts, or any combination thereof. In some embodiments, the one or more mobile device applications **127** are provided by third parties through which the mobile device applications **127** or user financial data may be accessed or managed. The mobile device applications **127** may include third-party applications, services and websites, web browser applications, social networking media, email servers and the like.

[0040] The third-party systems **140** can be any computerized apparatus controlled or operated by third parties other than the financial institution. In some embodiments, the third-party systems **140** include any system that hosts some functions, services or applications that are installed on the user mobile device **120**, or that are accessed or used by the user **130** via the user mobile device **120**. In some embodiments, the third-party systems **140** may also provide tools or information to the financial institution for generating certain functionality features for the switch-off system **110**.

[0041] The switch-off system **110**, the user mobile device **120** and the third-party systems **140** are each operatively connected to the network **150** and in communication with

one another. The network **150** may include various networking interfaces, such as a LAN, a WAN, a global area network (e.g., the Internet), or a hybrid thereof.

[0042] In some embodiments, the switch-off system **110** receives an indication to perform a switch-off for the mobile device **120** of the user **130**. In some embodiments, the indication to perform a switch-off of the mobile device **120** of the user **130** is an indication that the mobile device is compromised and may include an indication that the user mobile device **120** is misplaced, lost, or misappropriated, that the mobile device applications **127** are accessed or used by an unauthorized person, and/or that the user mobile device **120** and a wearable device of the user **130** are not co-located. In some embodiments, the indication is reported by the user **130**, for example, through a call center of the financial institution. In other embodiments, the indication may be detected by the switch-off system **110**. In some embodiments, the indication to perform a switch-off for the mobile device **120** of the user **130** is triggered by an indication from the user that the ownership of the mobile device will transfer. In such an embodiment, a user may securely remove important personal information from the mobile device and uninstall the applications before the mobile device is transferred to a third party. In some embodiments, the user **130** may simply wish to perform a switch-off for the mobile device **120**, and therefore may send the notification to the system to perform the switch-off.

[0043] In some embodiments, the switch-off system **110** detects that the user mobile device **120** are compromised by determining if the mobile device **120** and a wearable device (not shown) of the user **130** are co-located. In such embodiments, the switch-off system **110** may include a proximity system (not shown), to locate the mobile device **120**, which may have a positioning device (not shown) including one or more proximity sensors and/or a global positioning system (GPS), or the like. The wearable device may be paired with the user mobile device **120** via a secure channel between the two devices over a short range wireless communication channel. In other embodiments, the wearable device may include a GPS device which the system switch-off system may use to co-locate the wearable device with the mobile device by monitoring the GPS coordinates of both devices. The switch-off system **110** may determine a geographic location of the mobile device **120** via the proximity system that is configured to use proximity sensors located at various locations throughout the world to detect the presence of the one or more proximity sensors associated with the mobile device **120**. Alternatively, triangulation of cellular signals transmitted from the mobile device **120**, may be used to identify the location of the mobile device **120**. The switch-off system **110** may determine a geographic location of the wearable device via the secure channel previously established.

[0044] The switch-off system **110**, after receiving the indication to perform a switch-off for the mobile device **120** of the user **130**, the system may identify one or more applications (i.e., the mobile device applications **127**) associated with the mobile device **120**. In some embodiments, identifying the one or more mobile device applications **127** includes comparing the device data provided by the user **130** with the device data archived in the database **119**.

[0045] After the one or more applications have been identified, the switch-off system **110** remotely accesses the mobile device **120** to perform the switch-off of the one or more applications that are compromised. In some embodiments, the system may establish one or more secure electronic communication channels between the switch-off system **110** and the mobile device **120** of the user **130**. Each secure electronic communication channel allows the switch-off system to send signals to the mobile device which cause the mobile device to take certain actions, such as opening an application, logging out of an application, logging into an application, uninstalling an application, reconfiguring an application, installing an application, send messages, and the like. Additionally, the secure electronic communication channels allow the switch-off system to receive communications from the mobile device such as notifications regarding the status of the mobile device and applications associated with the mobile device, and the like.

[0046] In some embodiments, the switch-off is implemented by logging the user **130** (or a current user who is unauthorized to use the mobile device) out of the one or more applications. In some embodiments, at least one of the one or more applications is not currently open on the mobile device. In such embodiments, the system may transmit signals to the mobile device to cause the unopened applications to open or load on the mobile device before the system then logs the user out of the application. In some embodiments, switch-off is implemented by force closing the applications. In one embodiment, the system is executed on the mobile device **120** itself, and therefore the system does not need to remotely access the mobile device. In such an embodiment, at least a portion of the system may comprise an application stored on the mobile device **120** of the user **130**.

[0047] In some embodiments, after having performed a switch-off, the switch-off system **110** may go on to uninstall or reconfigure the one or more applications on the mobile device **120**, wherein uninstalling includes removing all or part of the compromised applications and reconfiguring involves disabling access to the applications. In some embodiments, prior to uninstalling or reconfiguring, the switch-off system **110** remotely accesses the mobile device **120** again to confirm that the switch-off is complete. In some embodiments, the system may additionally remove some or all cached data on the mobile device, lock one or more applications that still remain on the mobile device, and the like. In some embodiments, the system continues to record geographical location data associated with the mobile device to monitor the location of the mobile device. In some embodiments, a camera feature of the mobile device may be utilized by the system to help in identifying the operator of the mobile device at the user's request.

[0048] In some embodiments, the switch-off system **110** may restore the mobile device **120** to an original state prior to the switch-off, if the mobile device **120** was found or at request by the user **130**. In some embodiments, the mobile device **120** is restored by reinstalling the one or more applications that were removed from the mobile device **120**.

[0049] In some embodiments, after having restored the mobile device **120**, the switch-off system **110** prompts the user **130** to provide authentication credentials required for access to the one or more applications that have been reinstalled on the mobile device **120**. Upon receiving the authentication credentials from the user **130**, the switch-off system **110** validates the authentication credentials and, based on validation, re-establishes the user access to the applications.

[0050] FIG. **2** illustrates a general process flow **200** for performing a switch-off on a mobile device, in accordance with an embodiment of the present invention. The process **200** can be executed by the switch-off system **110** in the system environment **100**, as shown in FIG. **1**.

[0051] The process **200** includes multiple steps, executable by a processor of a system, which may be controlled by a financial institution or other operating entity. The process **200** starts with Block **210** to receive an indication to perform a switch-off of a mobile device associated with a user. The user may be the owner of the mobile device or a person who is authorized to use the mobile device and access one or more of the applications. In some embodiments, the indication is reported by the user, for example, through a call center, online reporting center, or other notification system of the operating entity. In other embodiments, the indication may be detected by the system. In some embodiments, the indication that the mobile device of the user is compromised may include an indication that the user mobile device is misplaced, lost, or misappropriated, that the applications are accessed or used by an unauthorized person, and/or that the user mobile device and a wearable device of the user are not co-located. In some embodiments, the indication to perform the switch-off is an indication that ownership of the mobile device will transfer from the user to a third party.

[0052] In some embodiments, the system detects that the user mobile device is compromised by determining that the mobile device and a wearable device of the user are no longer co-located. In such embodiments, the system may include a proximity system that monitors global positioning systems (GPS) or the like, associated with both the mobile device and the wearable device. In some embodiments, the wearable device may be paired with the user mobile device via a secure channel between the two devices over a short range wireless communication channel.

[0053] Upon receipt of the indication, the process **200** progresses to Block **220** to identify one or more applications associated with the mobile device. In some embodiments, identifying the one or more applications includes comparing the device data provided by the user with the device data archived in the database associated with the switch-off system. In some embodiments, the system identifies the one or more applications by remotely accessing the mobile device and searching for applications installed on the mobile device. In some embodiments, the operating entity and the user will have an agreement in place beforehand that the user desires for specifically identified applications stored on the mobile device of the user to be protected by the system. In such embodiments, the system may store this information in a database, such as the switch-off system database, and retrieve the user-identified applications to be used in the remainder of the system.

[0054] The process **200** may then progress to Block **230** to perform a switch-off on the one or more applications on the compromised mobile device. In some embodiments, performing a switch-off includes logging the user out of the one or more applications. In some embodiments, some of the applications are currently open on the mobile device. In such embodiments, the system may enter the open applications, and log the user out of the user's profile for that application. In some embodiments, some of the applications are not currently open on the mobile device. In such embodiments, the system may open the application on the mobile device, enter the newly opened application, and log the user out of the application.

[0055] The term "log out," as used herein, refers to any process performed on the mobile device to close a program or application on the mobile device or reduce the level of authorization granted to a possessor of the mobile device. For instance, logging out of an application may comprise completely removing the user's credentials from the application such that the user must completely log back in, possibly with a username and password, before the user can access the application.

[0056] In some embodiments, after logging the user out of the one or more applications, the system may check each application to ensure that the user is logged out. If the system determines that the user is not logged out of an application, then the system may attempt to log the user out of the application again and/or notify the user of the inability to log out of the specific application.

[0057] In some embodiments, the switch-off may further comprise uninstalling or reconfiguring the one or more applications. The system may uninstall all, some, or none of the applications and, likewise, may reconfigure all, some, or none of the applications. As used herein, the term "uninstall" generally refers to removing all or part of the one or more applications from the mobile device. As used herein, the term "reconfigure" generally refers to disabling access to the one or more applications without uninstalling the reconfigured applications from the mobile device.

[0058] In some embodiments, logging out of an application may include adjusting the level of authorization the possessor of the mobile device has for accessing the application. For example, in an online banking application on the mobile device, the system may have multiple tiers of authorization for the user's access to the application, with the lowest level being a simple display of an account balance, a second tier which allows the user to transfer funds from one user-owned account to another user-owned account, and a third tier which allows the user to transfer funds from a user-owned account to a third-party account. The online banking application may only require a password to grant access to the first authorization tier, but may then require more complex or unique authorization keys to access the second and third tiers (e.g., security questions, biometric information, two-step verification codes, and the like). Of course, any possessor of the mobile device has access to whichever tier is currently authorized on the mobile device. Therefore, if the online banking application is currently in the third authorization tier when the system runs the switch-off, the system may enter the application, and reduce the level of authorization to the second authorization tier. In this manner, the system may protect the user's information in the online banking application by limiting the available features of the application, to levels that remain safe to the user, while still allowing the user to access the application at some authorization tier once the mobile device is back with the user and the application is restored on the mobile device. Of course, both the full log out and the tiered authorization log out embodiments may be used by the system, with different embodiments used for different applications.

[0059] The process **200** may additionally include Block **240**, where the system uninstalls or reconfigures the one or more applications on the mobile device, wherein uninstalling includes removing all or part of the applications that are

compromised and reconfiguring involves disabling access to the applications. To accomplish these tasks, the system may remotely access the mobile device, enter an applications manager program, and uninstall or reconfigure settings for at least some of the applications on the mobile device. The system may completely wipe the mobile device of all applications, or may select a predetermined number of applications to remove from the mobile device, at the recommendation or instructions of the user. In one embodiment, the system is executed on the mobile device itself, and therefore the system does not need to remotely access the mobile device. In such an embodiment, at least a portion of the system may comprise an application stored on the mobile device of the user.

[0060] In some embodiments, the system does not remove all applications, but instead restricts or blocks access to one or more applications such that a possessor of the mobile device cannot open the applications on the mobile device until the system un-restricts access to the applications. In such an embodiment, the system keeps one or more applications stored on the mobile device at all times, which allows the user to continue using the applications, once the mobile device is restored to its active state, without having to re-install the applications.

[0061] In some embodiments, the process **200** may include Block **250**, where the system notifies the user of the switch-off. In some embodiments, notifying the user may comprise sending an electronic notification to another device of the user, the other device being a second mobile device, a wearable device, a desktop computer, and the like. In some embodiments, notifying a user may comprise sending a physical email or calling a landline telephone associated with the user to confirm the occurrence of the switch-off.

[0062] It should be noted that the steps performed in Blocks **210-240** may be performed by the mobile device itself without the need to remotely access the mobile device. In such an embodiment, at least a portion of the system may comprise an application stored on the mobile device of the user. In some embodiments, all of the steps are performed externally to the mobile device, requiring the system to remotely access the mobile device to accomplish each step. Of course, any combination of internal and external operations of the system may be utilized by the system to accomplish the tasks described with regard to the process **200**.

[0063] In some embodiments, the mobile device can be restored to an original state prior to the switch-off, if the mobile device was found or at request by the user. FIG. **3** illustrates a general process flow **300** for restoring a mobile device, in accordance with an embodiment of the present invention. Generally, the system prompts the user for authentication credentials, and re-enables one or more features of the mobile device upon validation of the user's credentials.

[0064] As shown in FIG. **3**, the process **300** may include Block **310**, where the system receives an indication to restore the mobile device. In some embodiments, the notification is from the user, is received by the system, and indicates that the mobile device should be restored to its original state, or a similar state. In some embodiments, the notification is determined by the system through monitoring the positioning components of the mobile device and the wearable device of the user to determine that the two devices are co-located again. When the mobile device and the wearable device are co-located, the system may make a strong assumption that the user has possession of the mobile device again. Therefore, the system may automatically restore the mobile device by automatically following through the rest of the process **300** as soon as the co-located nature of the devices is determined.

[0065] In some embodiments, the process **300** includes Block **320**, where the system restores the mobile device to an original state prior to the switch-off. In some embodiments, restoring the mobile device is implemented by reinstalling the one or more applications that were removed from the mobile device. In such embodiments, the system may remotely access the mobile device, access an application store or other system that enables the downloading of mobile device applications, and installs the one or more applications that were previously removed by the system as part of the process **200** described above.

[0066] In some embodiments, restoring the mobile device is implemented by executing a second reconfiguration on the one or more applications that were reconfigured as part of the switch-off process **200**. As with reinstallation, the system may remotely access the mobile device, access an application of the mobile device that allows for the manipulation of application statuses, and reconfigure the applications to their original configurations such that the user may again gain access to the applications.

[0067] Upon completion of restoring the mobile device, the process **300** progresses to Block **330** to prompt the user to input authentication credentials required for access to the one or more applications. In some embodiments, the authentication credentials include a username, a username, a password, a passcode, a PIN, security questions, and a biometric indicia, device info associated with the mobile device, the user account information, or any combination thereof.

[0068] As described above, with reference to Block **230** of FIG. **2**, the system may prompt the user to input one or more authentication credentials required for access to one or more authentication tiers for each of the one or more applications. For example, the system may detect that one of the applications that the system previously shut down had three authentication tiers, and the system logged the user out of the second and third authentication tiers before uninstalling the application. The system may then, upon re-installing the application, provide the user with the option to provide authentication credentials for the second authentication tier or the third authentication tier. In this manner, the system allows the user the opportunity to quickly re-establish the desired authentication tier for each of the one or more applications that the system logged the user out of during the switch-off.

[0069] In some embodiments, the process **300** includes Block **340**, where the system receives the required authentication credentials from the user for each of the one or more newly re-installed applications. The system may receive these authentication credentials via the mobile device itself, or through an alternate means of communication with the user. In some embodiments, the authentication credentials may be the same credentials for all applications. For example, the system may have determined the highest level of authentication credentials in use by the user at the time of the switch-off, and request that the user provide the same authentication credentials to allow the system to log the user back into each of the one or more newly re-installed applications. In this manner, the system may allow the user to

resume use of the mobile device in a substantially similar fashion as to the moment before the switch-off occurred, through the input of only one set of authentication credentials.

[0070] In another embodiment, the system may require that the user provide authentication credentials for each of the one or more applications that were logged out of during the switch-off. For example, if the system logged the user out of ten applications in the switch-off, then the system may require the user to provide authentication credentials for all ten newly re-installed applications.

[0071] In some embodiments, the system may determine the authentication credentials required for each of the one or more applications that the system logs the user out of as part of the switch-off. The system may then group the one or more applications of the mobile device by their required authentication credentials, and allow the user to provide each set of authentication credentials a single time, where each set of authentication credentials allows the system to give the user access to each application with that same set of authentication credentials. Of course, any combination of the example embodiments of authentication credentials and tiers of authentication may be used by the system.

[0072] In some embodiments, the process **300** involves Block **350**, where the system validates the authentication credentials of the user for each application. In some embodiments, the system has a database of stored authentication credentials based on previous input and/or requests from the user. In some embodiments, the system determines authentication credentials as part of the switch-off process. In such embodiments, the system may store the required authentication for each application in an electronic database. The system may then check the received authentication credentials with the stored authentication credentials to determine if the user's authentication credentials should be validated. In some embodiments, the system validates some authentication credentials, but not other authentication credentials.

[0073] For each validated application, the process **300** may include Block **360**, where the system re-establishes the user's access to the application on the mobile device of the user. Of course, the user's access to each application may be based on the authentication tier to which the user provided authentication credentials, or on which authentication tier the user was in at the time of the switch-off.

[0074] While the foregoing disclosure discusses illustrative embodiments, it should be noted that various changes and modifications could be made herein without departing from the scope of the described aspects and/or embodiments as defined by the appended claims. Furthermore, although elements of the described aspects and/or embodiments may be described or claimed in the singular, the plural is contemplated unless limitation to the singular is explicitly stated. Additionally, all or a portion of any embodiment may be utilized with all or a portion of any other embodiment, unless stated otherwise. In this regard, the term "processor" and "processing device" are terms that are intended to be used interchangeably herein and features and functionality assigned to a processor or processing device of one embodiment are intended to be applicable to or utilized with all or a portion of any other embodiment, unless stated otherwise.

[0075] Although a number of implementations have been described in detail above, other modifications, variations and implementations are possible in light of the foregoing teaching. The terminology used herein is for the purpose of describing particular embodiments only and is not intended to be limiting of embodiments of the disclosure. As used herein, the singular forms "a," "an," and "the" are intended to include the plural forms as well, unless the context clearly indicates otherwise. As used herein, all numbers may be read as if prefaced by the term "about," even if the term does not expressly appear. Also, any numerical range recited herein is intended to include all sub-ranges subsumed therein. It will be further understood that the terms "comprises" and/or "comprising," when used in this specification, specify the presence of stated features, integers, steps, operations, elements, and/or components, but do not preclude the presence or addition of one or more other features, integers, steps, operations, elements, components, and/or groups thereof.

[0076] The corresponding structures, materials, acts, and equivalents of all means or step plus function elements in the claims below are intended to include any structure, material, or act for performing the function in combination with other claimed elements as specifically claimed. The description of the present disclosure has been presented for purposes of illustration and description, but is not intended to be exhaustive or limited to embodiments of the disclosure in the form disclosed. Many modifications and variations will be apparent to those of ordinary skill in the art without departing from the scope and spirit of embodiments of the disclosure. The embodiment was chosen and described in order to best explain the principles of embodiments of the disclosure and the practical application, and to enable others of ordinary skill in the art to understand embodiments of the disclosure for various embodiments with various modifications as are suited to the particular use contemplated. Although specific embodiments have been illustrated and described herein, those of ordinary skill in the art appreciate that any arrangement which is calculated to achieve the same purpose may be substituted for the specific embodiments shown and that embodiments of the disclosure have other applications in other environments. This application is intended to cover any adaptations or variations of the present disclosure. Thus, although not expressly described, any or each of the features of the invention disclosed herein may be combined in any manner.

[0077] Accordingly, the invention is to be defined not by the preceding illustrative description but instead by the scope of the following claims.

INCORPORATION BY REFERENCE

[0078] To supplement the present disclosure, this application further incorporates entirely by reference the following commonly assigned patent applications:

Docket Number	U.S. Patent Application Ser. No.	Title	Filed On
6017US1CIP1.014033.2560	To be assigned	DETERMINING USER AUTHENTICATION BASED ON USER/DEVICE INTERACTION	Concurrently herewith

-continued

Docket Number	U.S. Patent Application Ser. No.	Title	Filed On
6017US1CIP2.014033.2561	To be assigned	DETERMINING USER AUTHENTICATION BASED ON USER PATTERNS WITHIN APPLICATION	Concurrently herewith
6929US1.014033.2562	To be assigned	PASSIVE BASED SECURITY ESCALATION TO SHUT OFF OF APPLICATION BASED ON RULES EVENT TRIGGERING	Concurrently herewith
6930US1.014033.2563	To be assigned	PERMANENTLY AFFIXED UNDECRYPTABLE IDENTIFIER ASSOCIATED WITH MOBILE DEVICE	Concurrently herewith
6933US1.014033.2565	To be assigned	TIERED IDENTIFICATION FEDERATED AUTHENTICATION NETWORK SYSTEM	Concurrently herewith

What is claimed is:

1. A system for integrated full and partial shutdown application programming interface, the system comprising:

a computer apparatus comprising at least one processor and a memory; and

a software module, stored in the memory, comprising computer readable code, executable by the processor, and configured to:

receive an indication to perform a switch-off for a mobile device associated with a user;

identify one or more applications associated with the mobile device; and

remotely access the mobile device to perform the switch-off of the one or more applications, wherein the switch-off comprises:

logging the user out of the one or more applications; and

uninstalling or reconfiguring the one or more applications from the mobile device, wherein uninstalling comprises removing all or part of the one or more applications from the mobile device, and wherein reconfiguring comprises disabling access to the one or more applications.

2. The system of claim **1**, wherein the switch-off further comprises confirming that the user is logged out of the one or more applications prior to uninstalling or reconfiguring the one or more applications from the mobile device.

3. The system of claim **1**, wherein the software module is further configure to:

restore the mobile device to an original state, wherein the original state is a state prior to the switch-off, wherein restoring comprises reinstalling the all or part of the one or more applications that were removed from the mobile device;

prompt, following restoring the mobile device, the user to input authentication credentials required for access to the one or more applications;

receive, from the user, the required authentication credentials;

validate the authentication credentials; and

re-establish, based on validating the authentication credentials, the user's access to the one or more applications.

4. The system of claim **3**, wherein the authentication credentials comprise one or more of a username, a password, a passcode, a personal identification number (PIN), security questions, biometric indicia, device info associated with the mobile device, and financial account information of the user.

5. The system of claim **1**, wherein the software module is further configured to notify the user of the switch-off.

6. The system of claim **1**, wherein the indication to perform the switch-off comprises an indication that the mobile device is misplaced or lost, that the one or more applications are misappropriated, or that the mobile device and a wearable device of the user are not co-located.

7. The system of claim **1**, wherein logging the user out of the one or more applications comprises logging the user out of a first authentication tier but not logging the user out of a second authentication tier.

8. A computer-implemented method for integrated full and partial shutdown application programming interface, the computer-implemented method comprising:

receiving an indication to perform a switch-off for a mobile device associated with a user;

identifying one or more applications associated with the mobile device; and

remotely accessing the mobile device to perform a switch-off of the one or more applications, wherein the switch-off comprises:

logging the user out of the one or more applications; and

uninstalling or reconfiguring the one or more applications from the mobile device, wherein uninstalling comprises removing all or part of the one or more applications from the mobile device, and wherein reconfiguring comprises disabling access to the one or more applications.

9. The computer-implemented method of claim **8**, wherein the switch-off further comprises confirming that the user is logged out of the one or more applications prior to uninstalling or reconfiguring the one or more applications from the mobile device.

10. The computer-implemented method of claim **8**, wherein the computer-implemented method further comprises:

restoring the mobile device to an original state prior to the switch-off, wherein the original state is a state prior to the switch-off, and wherein restoring comprises reinstalling the all or part of the one or more applications that were removed from the mobile device;

prompting, following restoring the mobile, the user to input authentication credentials required for access to the one or more applications;

receiving, from the user, the required authentication credentials;

validating the authentication credentials; and

re-establishing, based on validating the authentication credentials, the user's access to the one or more applications.

11. The computer-implemented method of claim **10**, wherein the authentication credentials comprise one or more of a username, a password, a passcode, a personal identification number (PIN), security questions, biometric indicia, device info associated with the mobile device, and financial account information of the user.

12. The computer-implemented method of claim **8**, wherein the computer-implemented method further comprises notifying the user of the switch-off.

13. The computer-implemented method of claim **8**, wherein the indication to perform the switch-off comprises an indication that the mobile device is misplaced or lost, that the one or more applications are misappropriated, or that the mobile device and a wearable device of the user are not co-located.

14. The computer-implemented method of claim **8**, wherein logging the user out of the one or more applications comprises logging the user out of a first authentication tier but not logging the user out of a second authentication tier.

15. A computer program product for integrated full and partial shutdown application programming interface, the computer program product comprising a non-transitory computer readable medium having one or more computer-readable programs stored therein, and the computer readable programs, when executed by a computer apparatus, cause the computer apparatus to perform the following steps:

receive, via a computing device processor, an indication to perform a switch-off for a mobile device associated with a user;

identify, via a computing device processor, one or more applications associated with the mobile device; and

remotely access, via a computing device processor, the mobile device to perform the switch-off of the one or more applications, wherein the switch-off comprises:

logging the user out of the one or more applications; and

uninstalling or reconfiguring the one or more applications from the mobile device, wherein uninstalling comprises removing all or part of the one or more applications from the mobile device, and wherein reconfiguring comprises disabling access to the one or more applications.

16. The computer program product of claim **15**, wherein the switch-off further comprises confirming that the user is logged out of the one or more applications prior to uninstalling or reconfiguring the one or more applications from the mobile device.

17. The computer program product of claim **15**, wherein the computer readable programs cause the computer apparatus to:

restore, via a computing device processor, the mobile device to an original state, wherein the original state is a state prior to the switch-off, wherein restoring comprises reinstalling the all or part of the one or more applications that were removed from the mobile device;

prompt, via a computing device processor, following restoring the mobile device, the user to input authentication credentials required for access to the one or more applications;

receive, via a computing device processor, from the user, the required authentication credentials;

validate, via a computing device processor, the authentication credentials; and

re-establish, based on validating the authentication credentials, the user's access to the one or more applications.

18. The computer program product of claim **17**, wherein the authentication credentials comprise one or more of a username, a password, a passcode, a personal identification number (PIN), security questions, biometric indicia, device info associated with the mobile device, and financial account information of the user.

19. The computer program product of claim **15**, wherein the computer readable programs cause the computer apparatus to notify, via a computing device processor, the user of the switch-off.

20. The computer program product of claim **15**, wherein logging the user out of the one or more applications comprises logging the user out of a first authentication tier but not logging the user out of a second authentication tier.

* * * * *